

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28

2
3
4
5
6
7
8
9
10
11
12
13
14

16

17
18
19
20
21

23
24
25

1 4. The method of claim 1 wherein the unfolded transport key
2 has a volume equal to twice the volume of the previous transport
3 key.

4 5. The method of claim 1 wherein the unfolding step is the
5 reverse of a key folding process using bit swapping.

6 6. The method of claim 5 wherein the unfolding is performed
7 by:
8

9 splitting each byte of the previous transport key into
10 two new bytes;

11 moving most significant bits of each byte of the
12 previous transport key into least significant bits
13 of a new byte of the unfolded transport key; and
14 padding the most significant bits of each new byte of
15 the unfolded transport key with identical bits.
16

17 7. The method of claim 1 wherein the unfolding step
18 comprises expanding by a factor of two the size of the previous
19 transport key by means of concatenating a common MSB sequence at
20 uniform intervals throughout the length of said previous
21 transport key.

22 8. The method of claim 1 wherein the unfolded transport key
23 comprises bytes from a range of consecutive bytes from an ASCII
24 character set.
25
26
27
28

1 9. The method of claim 8 wherein the consecutive bytes from
2 the ASCII character set are the sixteen consecutive bytes from
3 the ASCII character set 64 (decimal) through 79 (decimal).

4 10. The method of claim 1 wherein the cryptographic key is
5 adapted for use in a One-Time Pad cipher system.
6

7 11. The method of claim 1 wherein the encrypting step and
8 the decrypting step are performed using the same key.

9 12. The method of claim 1 wherein:

10 the steps of combining, unfolding, encrypting,
11 distributing, and decrypting are repeated a
12 plurality of iterations; and

13 the transport key from a given iteration is used to
14 create the unfolded transport key used in the
15 encrypting and decrypting steps in a subsequent
16 iteration.
17

18 13. The method of claim 12 wherein the repetition of the
19 combining, unfolding, encrypting, distributing, and decrypting
20 steps is terminated after a preselected event has occurred.

21 14. The method of claim 1 wherein the encrypting step is
22 performed using an encryption key consisting of the unfolded
23 transport key XORed with a conversion key.
24

25 15. The method of claim 14 wherein the conversion key is a
26 subset of the cryptographic key.
27
28

1 16. The method of claim 14 wherein the conversion key is
2 generated by a true random number generator.

3 17. The method of claim 14 wherein the conversion key
4 converts the unfolded transport key into a key whose bytes span a
5 full range of an ASCII character set.

6 18. A computer-readable medium containing computer program
7 instructions for securely distributing a cryptographic key, said
8 computer program instructions performing the steps of:

9 combining the cryptographic key with a fresh transport
10 key to form a key set;
11 unfolding a previous transport key to form an unfolded
12 transport key;
13 encrypting the key set using the unfolded transport key
14 to form an encrypted key set; and
15 distributing the encrypted key set across a medium.

16 19. Apparatus for securely distributing a cryptographic key
17 from a first party to a second party, said apparatus comprising:

18 means for generating the cryptographic key;
19 means for generating a fresh transport key;
20 means for unfolding a previous transport key to form an
21 unfolded transport key;
22 means for encrypting the cryptographic key and the
23 transport key using the unfolded transport key to
24 form an encrypted key set; and
25 distributing the encrypted key set across a medium.

1 means for enabling the first party to distribute the
2 encrypted key set across a medium to the second
3 party.

4 20. Apparatus of claim 19 further comprising means for
5 XORing the unfolded transport key with a conversion key to create
6 an encryption key, wherein the encryption key encrypts the
7 cryptographic key and the transport key.
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28